UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,637	07/06/2001	Uwe Hansmann	DE920000036US1	7571

7590 09/27/2004

WILLIAM KINNAMAN, JR.
IBM Corporation
Intellectual Property Law Department
2455 South Road, M/S P386
Poughkeepsie, NY 12601

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/900,637	HANSMANN ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 have been examined.

Specification

2. The abstract of the disclosure is objected to because it exceeds 150 words in length. Correction is required. See MPEP § 608.01(b).

Claim Objections

3. Claim 12 is objected to because of the following informalities: change "smartcard" (3rd line) to "said smartcard" and "receiving device" (3rd line) to "said receiving device". Claims that are not specifically addressed are objected to by virtue of their dependencies. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 10, 12 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 10, claim 1 is written such that the method as a whole and the comparing step in particular can only be accomplished by the receiving device. Therefore, the claim language does not support the added limitation in claim 10. For

examination purpose, the claim is interpreted as further comprising the steps of receiving a hash by the sending device from the receiving device and comparing said hash received from said receiving device with a hash of said sending device, wherein both hashes are calculated by hash algorithms using identification data and said common secret.

b. Regarding claim 12, it recites the limitation "said comparing component of said sending device" in the 2nd line. There is insufficient antecedent basis for this limitation in the claim. There is no component in the claim, and it is the receiving device, not the sending device, that performs the comparing step. The limitation is interpreted as "a comparing component of said sending device". Claims that are not specifically addressed are rejected to by virtue of their dependencies

c. Regarding claim 16, it recites the limitation "said client is a portable device". There is insufficient antecedent basis for this limitation in the claim. The limitation is interpreted as "said sending device is a portable device".

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-7, 9, 11, 14-15 and 18-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Atalla (4,283,599).

a. Regarding claim 1 which is representative of claims 18-20, Atalla discloses a method for authentication of communicating devices having a common secret, said method comprising the steps of:

receiving a hash by a receiving device from a sending device (figures 1A-1B); and

comparing said hash received from said sending device with a hash of said receiving device, wherein both hashes are calculated by hash algorithms using a random number, which meets the limitation of identification data, and said common secret (figures 1A-1B and corresponding sections in specification).

b. Regarding claim 2, Atalla further discloses that said identification data is generated by said sending device (figures 1A-1B).

c. Regarding claim 3, Atalla further discloses that said identification data is sent from said sending device to said receiving device (figures 1A-1B).

d. Regarding claim 4, Atalla further discloses that said hash algorithms are identical (col. 3, lines 36-38).

e. Regarding claim 5, Atalla further discloses that said common secret comprises a PIN (figures 1A-1B).

f. Regarding claim 6, Atalla further discloses that said common secret comprises a PIN (figures 1A-1B) which meets the limitation of a password.

g. Claim 7 is rejected on the same basis as claim 1.

h. Regarding claim 9, Atalla further discloses that said random number is generated by a random number generator which is part of said sending device (fig. 1A). Atalla does not explicitly disclose that the random number generator is a software component; however, software and hardware are logically equivalent.

i. Regarding claim 11, Atalla further discloses that said comparing step is accomplished by said receiving device (fig. 1A).

j. Regarding claim 14, Atalla further discloses that the data connection between the sending device and the receiving device is an insecure data connection (see Abstract).

k. Regarding claim 15, Atalla further discloses that said sending device and said receiving device form a client-server architecture (fig. 1B).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla as applied to claim 7 above, and further in view of Heinz, Sr. (5, 812,764). Atalla does not disclose that the random number is generated by an operating system of said sending device. Heinz discloses a random number is generated by an operating system (col. 5, lines 41-45). It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify the Atalla method such that the random number is generated by an operating system, as taught by Heinz. The motivation for doing so would have been to utilize the built-in random-number generating function of the operating system.

10. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla as applied to claim 1 above, and further in view of Kaufman et al. (Network Security – Private Communication in a Public World). Atalla does not disclose the steps of receiving a hash by the sending device from the receiving device and comparing said hash received from said receiving device with a hash of said sending device, wherein both hashes are calculated by hash algorithms using identification data and said common secret. Kaufman discloses an authentication method that the steps of receiving a hash and comparing the received hash with a generated hash are performed at both ends of a communications channel (see p. 107, Section 4.2.1 Authentication). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Atalla method such that the steps of receiving a hash and comparing the received hash with a generated hash are performed at both ends, as taught by Kaufman, to achieve mutual authentication.

11. Claims 12-13 and 16 rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla as applied to claim 1 above, and further in view of Aiello et al. (6,496,808).

a. Regarding claim 12, Atalla does not disclose utilizing a smart card such that said common secret, said hash algorithm and a comparing component of said sending device are stored in the smart card and communication between the smart card and the receiving device is established via a card reader. Aiello discloses utilizing a smart card for authentication purpose, the smart card having a common secret stored in its secure memory, a hash algorithm and a comparing component (col. 9, lines 49-54; col. 10, lines 4-10 and 42-44). Aiello also discloses that communication between the smart card and the receiving device is established via a card reader (figures 1 and 5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Atalla method to utilize a smart card such that said common secret, said hash algorithm and a comparing component of said sending device are stored in a smart card and communication between the smart card and the receiving device is established via a card reader, as taught by Aiello. The smart card permits a user to conduct remote transactions while using an untrusted computing device (col. 1, lines 53-56).

b. Regarding claims 13 and 16, Atalla does not discloses that the sending device is a portable device having the smart card and the smart card reader. Aiello discloses a portable sending device having the smart card and the smart card reader (col. 3, lines 31-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Atalla such that sending device is a portable device having the smart card and the smart card reader, as taught by Aiello. People can carry

portable devices in their pockets and use them at all times to perform financial transactions (col. 1, lines 38-44).

12. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla in view of Kaufman. Atalla discloses a client-server architecture in which the server performs the authentication method of claim 1 (figures 1A-1B). Atalla does not disclose that the client authenticates the server. Kaufman discloses a system in which authentication is performed at both ends (fig. 3). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Atalla architecture such that the client also performs the authentication, as taught by Kaufman, to achieve mutual authentication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
9/20/04

Gilberto Barron

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100